LLNL-CONF-675921

# University Research Test Reactor (RTR) - A Security Challenge

S. Porter

August 5, 2015

University Research Test Reactor (RTR) # A Security
Challenge
Vienna, Austria
November 16, 2015 through November 20, 2015

## Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

# University Research Test Reactor (RTR) – A Security Challenge

**International Atomic Energy Agency, November 16-20, 2015**

**Author:** Stephen J. Porter[1]
[1]Lawrence Livermore National Laboratory, Livermore, California, USA
E-Mail: porter16@llnl.gov

## ABSTRACT

Research Test Reactors (RTR) by their design and purpose are often co-located within college or university campuses. This makes them a challenge to secure in such an open environment, while concurrently providing access to those who need to use them for research and testing. One such RTR, which is the focus of this paper, is located at a prominent university within the United States. Like most college campuses the student population is made up of domestic and international students, as well as a diverse faculty and staff. Moreover, adding to the security and safety risk, the RTR is situated adjacent to the university's sports stadium. So in addition to the existing campus population, the location of the RTR posed even a greater threat to a large number of concentrated attendees during sporting events. After performing a thorough assessment of the RTR, it was evident the majority of the antiquated physical security system needed replacing, as well as revamping its access control by introducing a multilayered and multifactor approach. Biometric authentication was also added as an additional factor for access to the target; as well as ensuring tightly managed ACLs (Access Control Lists). The existing safety interlocking portals were also security enhanced. The RTR and associated entry points encompassed several buildings, as well as vehicle access points. Once critical pathways were identified, nested security zones along with external controls were incorporated into the overall design. Moreover, a separate dedicated secure LAN (Local Area Network) was considered for the RTR security system, in lieu of a VLAN (Virtual LAN) that would ride on the existing unsecure university's network backbone. Through many secure discussions, design reviews, and modifications, the final design was accepted and incorporated, allowing the RTR to operate in a much more secure and safe manner within the campus community.

## BACKGROUND

During the 1950's and 60's research and test reactors (RTRs) were constructed throughout the United States, with most being co-located at universities. The U.S. Nuclear Regulatory Commission (NRC) regulates most RTRs, while others are managed by the Department of Energy. Given the average age of these RTR's, many were found to be in disrepair or in need of upgrades due to antiquated technologies. This includes the safeguards and security systems that were put in place to protect them. RTRs are not all of the same design, or type of nuclear fuel used, or output power capacity.

RTRs with power outputs greater than 2000 kW are classified as high powered reactors and are used for major research. They are generally located at national laboratories or universities. These high power reactors perform vital research with regard to materials behavior under irradiation, isotope production for research and medicine, and provide high-flux neutron beams for research. Mid-Power RTRs, have power capacities from 250 to 2000 kW and are configurable, so they can perform a wide range of research activities including radiography, neutron beam research, neutron scattering, as well as neutron activation analysis (NAA). Low-Power RTRs (< 250 kW) are excellent for training operators and educating students, as well as radio-nuclear applications such as NAA.

The RTR which provides the basis of this discussion is a Low-Power RTR with a power capacity of 100kW. This RTR was built in the late 50's and was one of the first research test reactors to be constructed on a university campus. The reactor is an Argonaut graphite moderated/ amber reflected design that is used for education, training, nuclear research, testing, and related activities. Like many research test reactors, it was down-converted to use lower enriched uranium (LEU), after the Nuclear Regulatory Commission changed regulations for all its training reactors following 9/11. The reactor's power level is regulated by cadmium blades, with its nominal maximum thermal flux density at 1.8E12 neutrons/cm$^2$·s.

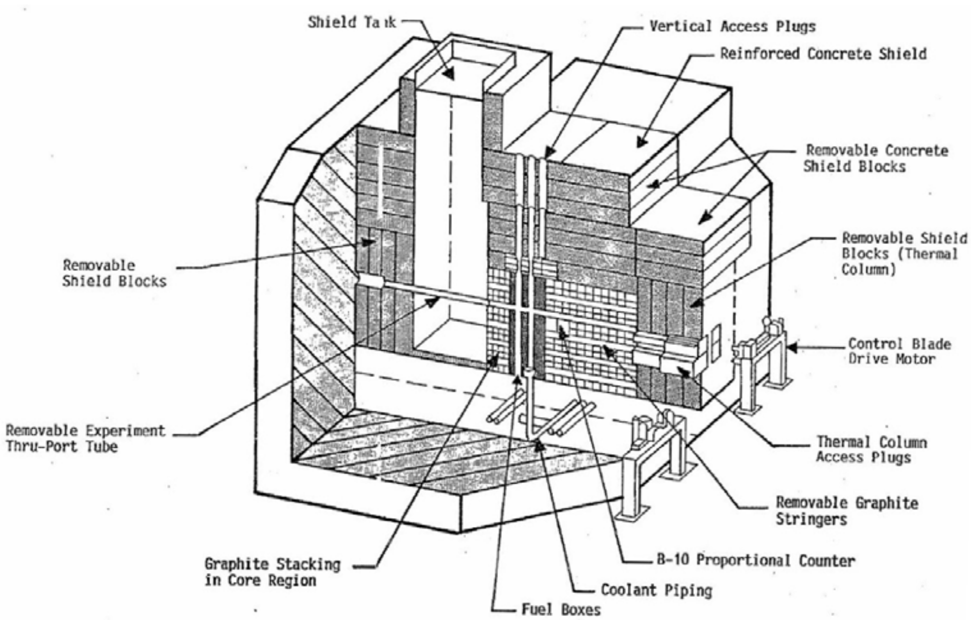
Shield Tank
Vertical Access Plugs
Reinforced Concrete Shield
Removable Concrete Shield Blocks
Removable Shield Blocks (Thermal Column)
Removable Shield Blocks
Control Blade Drive Motor
Removable Experiment Thru-Port Tube
Thermal Column Access Plugs
Removable Graphite Stringers
B-10 Proportional Counter
Graphite Stacking in Core Region
Coolant Piping
Fuel Boxes

**Figure 1. Argonaut Research Test Reactor**

Compliance with the NRC had been grandfathered in YOY, however, due to operating and security concerns the RTR was taken out of service in in 2007. It was off line for eight years after undergoing a multi-year facility refurbishment that included upgrades to the physical infrastructure, nuclear control and instrumentation (C&I) systems, HVAC systems, reactor instrumentation sub-system, safeguards, and physical security systems, which will be explored further in this discussion.

## THE CHALLENGE

Given the reactor's age and its overall degradation through the years (due in large part to a lack of funding), presented a challenge to keep the reactor operational, safe, and secure. This included outdated components, many of them analog, which made up the physical security system, and degraded infrastructure which provided the backbone (network) for the PPS. To add to the security challenge, through the years the university campus had built up around the RTR. The growth also spawned a new sports complex which included a stadium located close to the RTR. The stadium often sees over 90K in attendance during sporting events.

Moreover, as it is with most universities both the student population and university faculty is very diverse, including foreign nationals. This diversity of students and faculty is very welcome in academia, but does pose a 'potential' security threat with respect to nefarious actions by individual(s) or their possible allegiances or alliances with foreign or domestic terrorist groups. We were told there were no foreign nationals on the managed ACL (Access Control Lists) for entering the reactor room itself; however, some of the adjacent rooms were not as tightly controlled. While performing a security out-brief in one of the RTR facility meeting rooms to the university's RSO (Radiation Safety Officer), Reactor Director, security staff, and agents from the FBI - a university professor with unfettered access along with his students that included foreign nationals entered the room during the out-brief while we were discussing vulnerabilities. This accentuated the point that was being made regarding managing access.

The RTR and supporting facilities were all housed in multi-story buildings which were interconnected with each other and also connected to other campus buildings. Of course, relocating the RTR and its associated facilities was not going to be an option, nor was the multi-million sports complex including the massive stadium going to move. A Hot Cell was also housed near the reactor in another room used to handle other radiological sources. All of the interconnected buildings added to the number of critical pathways and potential access points that needed to be addressed.

## ASSESSMENT

Using a standard set of criteria regarding attractiveness of material and guidelines for protection; a team made up of physical protection experts and university stakeholders including the Reactor Director, Sr. Reactor Operator, RSO, Security Director, IT staff, and other SME's performed a thorough assessment of the RTR facilities and the university's overall security protection.

As it is with most institutions or businesses - changes to facilities, and turnover in management and personnel is a recurring theme. This scenario was no different as the Reactor Director was leaving for another position, the university was getting ready to upgrade major parts of its security system, and there were planned changes for the RTR facility itself.

These changes actually presented an opportunity to integrate much needed leading edge PPS upgrades, and much needed improvements to the overall security scheme and culture.

With this being an NRC regulated facility; the NRC was kept informed regarding results of the assessment, and apprised of suggested security changes. The NRC was very supportive and involved, especially within their areas of expertise regarding safeguards and reactor improvements. The NRC was known to be leery of replacing all the analog components with digital upgrades, and preferred to stay analog where possible. We were directed to 10 CFR 50.59 that addressed Changes to Facilities, Procedures and Tests, which stated security effectiveness could not be reduced due to changes. Of course we were looking to achieve just the opposite, that is, to enhance security operations.

Regarding the physical aspects of the RTR facilities and adjoining buildings, the assessment revealed several unsecured points of entry (POE). Though perimeter doors were kept locked and checked every day, some were not alarmed. There were also several unsecured vents, including a HVAC ventilation room located right next to the reactor room with a cavity large enough to climb through and gain access to the reactor itself. The parking lot entry to the RTR facility was fenced in and controlled with only a mechanical lock. Surrounding the chain link fence were decorative boulders used as physical barriers, however, their spacing was inadequate to stop a vehcile.

There was a security system dedicated to the RTR which employed some redundancy, however, the technology was outdated and nearing its EOL (End of service Life). Alarms were ported to the university's SCC (Security Command Center), but not only were there numerous false and nuisance alarms reported, the SCC itself was poorly secured (addressed separately as part of the university's overall security assessment). A standalone DB (database) was set up for managing ACLs (Access Control Lists), but the technology stack was also nearing EOL. Radiation portal monitors were in place, but they were also outdated and poorly maintained. In addition, not all of the PPS external contractor support personnel underwent FBI background checks. Foreign nationals were not on the ACLs, and they did require escort for access.

Additional observations:

- Manual bollards to RTR driveway, but only used during major sporting events
- Analog phone for security reporting - service was extremely intermittent/ antiquated
- Mobile duress was available, but tied to the outdated unreliable security system (PPS)
- NO POE (Point of Entry) assessment cameras
- University Police Department (UPD) did not have access to the reactor bay
- Physical keys for TPC, controlled by Reactor Director, special order blanks
- RTR roof was thinly constructed
- Not all cameras were operational, including the one inside covering the main entry door
- Diesel generator backed up part of the PPS, but not for all components or subsystems

- No man bars on the vents, including HVAC cavity
- Short walls, that were open above the hung ceilings
- Shielding was the only delay to the reactor source material
- Insufficient lighting

Most RTR personnel had background checks which included FBI check and fingerprinting to deem them Trustworthy and Reliable (T&R). NRC 10 CFR 73.56 was complied with for determining personnel access authorization requirements, which called for verification of true identity, employment history evaluation, credit history, character and reputation evaluation, criminal history, psychological assessment, and other criteria. But not all those responsible for the RTR support systems had T&R background checks.

Infrastructure that provided the network backbone to the PPS was also assessed and found to have its own set of problems. The university, like many institutions use VLANS (Virtual Local Area Networks) to provide segmentation as a method to secure networks, however, VLANs still ride on institutional network hardware. The networks are managed by an IT staff that often does not have the same vetting (e.g. FBI background checks) as the PPS management and support staff. There was a PoP (Point of Presence) dedicated to the reactor building, that did provide an artificial demarcation or interface point between the RTR and the UPD SCC. Moreover, there were not enough firewalls in place to sufficiently provide protection, and the firewalls that were in place were not configured adequately. Some encryption methods were employed but they relied on the old AES 128 encryption method which was known to be inadequate.

Even the best intrusion detection systems (IDS) and delay built into the overall protection scheme are not enough if the response is not in a time, and/or the response force is ill-equipped to provide containment (primary goal). The response was graded against criteria that included response times, number of responders, and equipment (e.g. radios, weapons) with regard to primary, secondary, and tertiary response forces. The university had its own police department (UPD), but relied on the LLEA (Local Law Enforcement Agencies) if extra measures were needed. The LLEA had already established its own city and county Combined Call Center (CCC). The county also had its own trained SRT team (Special Response Team). These were definitely high marks regarding response attributes. The UPD and LLEA possessed adequate communication technologies, however, shared communication channels between the UPD and the LLEA had not been established.

## SOLUTIONS

To address all the aforementioned security issues and bring the RTR into compliance was a very involved and complex multi-year project. There were numerous obstacles and dependencies that had to be overcome in order to apply the best solutions. Upgrades to the RTR physical protection system and its associated sub-systems (e.g. database) were coordinated with the wholesale upgrades to the reactor bay and its control and instrumentation systems. In addition, the upgrades had to be compliant with the rest of the overall PPS upgrades, including the university's Security Command Center. Multiple design reviews were performed with all the various stakeholders, including the NRC. Results from a DBT (Design Basis Threat) were also considered for input to the overall design. It was also determined that only contractor's with personnel who had FBI background checks were allowed to bid for the work.

The intrusion detection subsystem (IDS) was completely refurbished, including the use of state of the art security components to provide true volumetric coverage. Alarm outputs were ported to the university's PPS through new secure fiber networks. The new PPS had its own LAN managed by a reduced set of IT personnel with background checks. The integrated access control system (ACS) was also redesigned to include multi-factor authentication, anti-passback, and nested areas closer to the target with additional authentication (e.g. biometrics). The ACLs (Access Control Lists) were tightly managed, while TPC (Two Person Control) was incorporated where needed. Per the Reactor Director's discretion the controlled mechanical keys were kept as part of the overall design for additional security.

Additional upgrades/ improvements:

- University's SCC (Security Command Center) was hardened as part of the university's overall security upgrades
- Man-bars installed on vents and in HVAC room
- Additional lighting installed for assessment, and overall safety and security
- Electro-mechanical pop up barrier, replaced the manual bollards
- Multi-factor authentication components (badge reader, keypad, iris-scan)
- New radiation portal monitors
- BMSs (Balanced Magnetic Switches) for all doors
- Dual tech (IR/ uW) motion detectors for volumetric coverage
- Local audible alarms - where appropriate
- Duress strips installed where needed
- Mobile duress devices distributed to RTR occupants
- Cameras with IR illuminators with alarm triggered presets (internal and external)
- Security controllers were placed inside secure area (high side)
- Security culture emphasized (e.g. operational security or OPSEC)

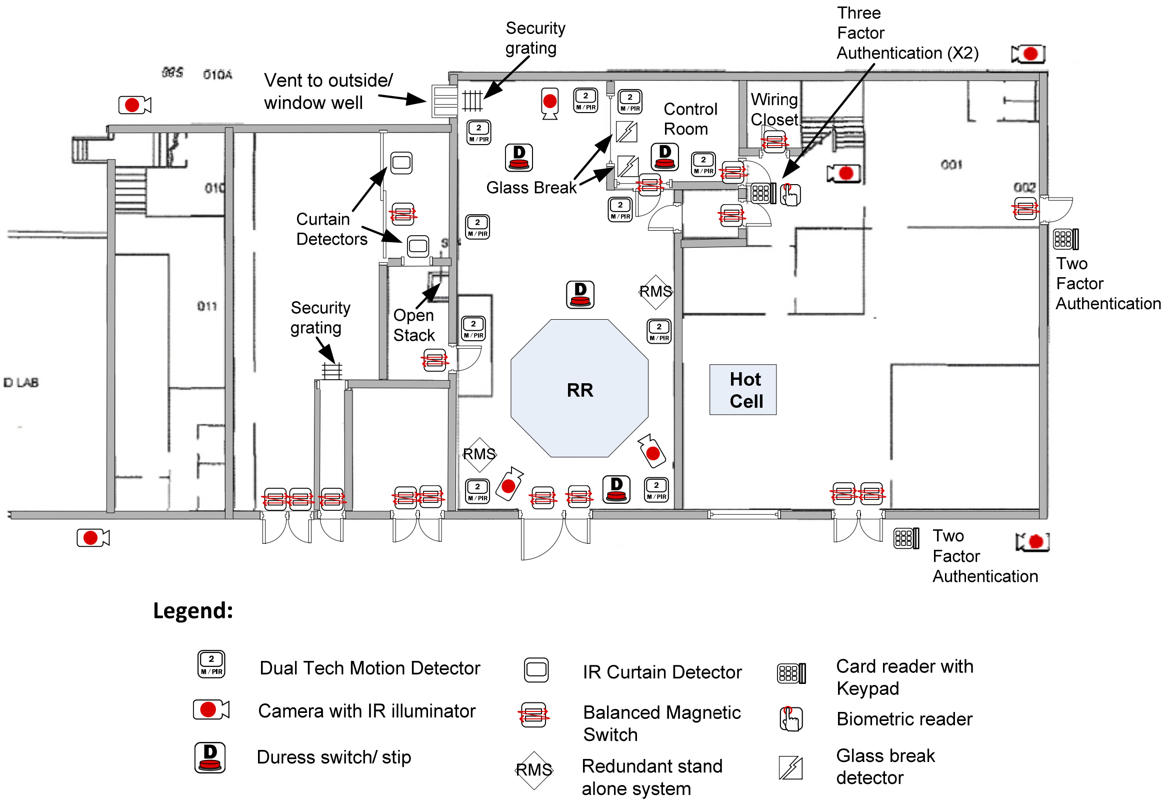

***Figure 2. Main RTR security upgrades***

The IT infrastructure was also updated including new network switches employing port security, core distribution routers, and additional firewalls used to create security zones or segments. A new 20Gb fiber backbone (network) was also installed to ensure there was enough bandwidth to support the new digital components, including IP camera video packets, and VoIP (Voice over IP) that was also incorporated into the design. Cyber security was also addressed (e.g. non-routable networks, complex passwords, redundancy, enhanced encryption, network scans). And most importantly the IT staff, as well as maintenance contractors providing support also underwent T&R background checks.

Even with all the new security enhancements to the institutional PPS, plus upgrades to the network infrastructure, and a trustworthy and reliable support staff, there was still a potential for attack paths that could render the PPS useless. Therefore a true redundant standalone system was included as part of the design, a small alarm system completely separate from the institutions security system and network infrastructure.

This redundant security system was solely dedicated to the protection of the target or reactor itself; therefore the alarms were limited to a subset including radiation detection, and a conductive alarm loop employing RFIDs around the reactor. The redundant system also has its own communication paths (e.g. dial up, cell service, and/or satellite), so in the event the institution's network is compromised such as a DOS (Denial of Service) attack, the redundant system fails over to its own alternate communication link. The redundant system's alarm outputs were monitored by the university's SCC, and monitored off-site at the LLEA CCC.

The response was also addressed after the thorough assessment of their capabilities. Additional radios were procured that would allow the UPD and LLEA to communicate on the same channels. Most of the patrol cars (motors) were equipped with mobile laptops with security application software capable of receiving alarms and detailed instructions. Memorandums of Understanding (MOUs) were either revisited or new ones written to address roles and responsibilities. Rules of engagement were also reviewed and updated (e.g. when to use deadly force), as well as compensatory measures in the event the PPS goes down.

The university's police department (UPD) along with the city and county LLEA, as well as the RSO and other key support staff (e.g. dispatchers) were put through alarm response training. Some fire department, hazmat, and emergency services personnel were also included or briefed where their services intersected. All stakeholders took the training together so they could create realistic settings and scenarios, stage responses, manage triage, and address gaps. In addition, the NRCs basic RAD 19 training was attended.

## MANAGEMENT • SUSTAINABILITY

Management and support of the Physical Protection System and associated sub-systems is as important as the upgrades to the systems themselves. Roles and responsibilities must be clearly defined regarding operations, support, and response, while policies, procedures, MOU's etc. need to be periodically reviewed and updated. Moreover, with so many interdependencies the PPS and IT staff need to remain in constant communication as they review security plans, configuration management, and address gaps.

The following items should be applied as a check and balance to help mitigate the divide between RTR operations, security management, PPS and IT support:

- Security self-assessments of both systems and networks
- Configuration management (keep current)
- Security Plans (review and update periodically, as well as before and after system upgrades)
- Approved equipment lists, including hardware, operating systems, application software, firmware, etc., and associated revision levels
- Map interdependencies between hardware, software, hosts, and subsystems
- End-to-end testing performed jointly before incorporating new code or technologies
- Procedures (kept current) for performing upgrades, including comprehensive checklists
- License management (e.g. some legacy software won't run on new platforms)
- Automated virus scans and patches
- Documentation control (make sure its kept current and secure)
- Manage ACL lists/ Security culture (OPSEC)
- Budget/ Training/ Spare Parts

There is much more to be said in the area of PPS management and sustainment, but it's in the application of these practices that makes the difference to ensure systems stay compliant, and compliance helps in the overall fight against security breaches.

## CONCLUSION

The research test reactor was taken off line and remained inactive for years as upgrades were performed on the reactor itself, the high bay, instrumentation & control systems (I&C), support facilities, and the safeguards and security systems. Following successful upgrades and ensuing inspections the RTR was brought back on line and is now providing research and training to academic institutions, government, and corporations (including future reactor operators) in areas such as: neutron activation analysis (NAA), neutron irradiation, radiation effects testing on materials, and partnerships in research. All in a safe and secure manner.

## REFERENCES

1. Nuclear Reactors Built, Being Built, or Planned, *Department of Energy Office of Nuclear Energy, Science and Technology, 2003*
2. Protection and Sustainability Criteria document, 2007, 2010. *Office of Global Threat Reduction, DOE NNSA*
3. Training Reactors designed by Argonne National Laboratory: ARGONAUT. *Argonne National Laboratory*. May 2, 2012.
4. Training Requirements for Radiation Workers; Title 10, Part 19, of the *Code of Federal Regulations* (10 CFR Part 19), ...
5. Physical Protection Systems and the Cyber Security Component, *Stephen J. Porter, Lawrence Livermore National Laboratory*, Livermore, California, USA, 2015
6. Position Statement #53, June 2011, *American Nuclear Society (ANS)*
7. Changes, tests and experiments, *NRC 10 CFR 50.59*
8. Personnel access authorization requirements for nuclear power plants, *NRC 10 CFR 73.56*

Prepared by LLNL under Contract DE-AC52-07NA27344.